

CLAIMS

What is claimed is:

1 1. A method comprising:
2 (a) generating a key hash result partially based on a global identifier of a
3 source and an estimated current time at the source;
4 (b) producing a first time-varying item based on the key hash result; and
5 (c) presenting the first time-varying item for comparison with a second
6 time-varying item being presented at the source.

1 2. The method of claim 1, wherein the presenting of the first time-varying
2 item is contemporaneous with presentation of the second time-varying item if the
3 global identifier of the source is accurately received and the current time at the source
4 has been accurately estimated.

1 3. The method of claim 1 further comprising:
2 (d) repeating (a), (b) and (c) for each subsequent presentation of a newly
3 produced first time-varying item and comparison of the newly produced first time-
4 varying item with a newly produced and presented second time-varying item.

1 4. The method of claim 3, wherein prior to generating the key hash result,
2 the method further comprises:
3 receiving a verification packet from the source, the verification packet including
4 the global identifier of the source and a local time value at which the verification packet
5 was formed at the source.

1 5. The method of claim 4, wherein the verification packet further includes
2 a table inclusive of items displayed as the first time-varying item and the second time-
3 varying item.

1 6. The method of claim 4, wherein the verification packet further includes
2 a data field to contain information to be transferred.

1 7. The method of claim 6, wherein the information includes a lookup table
2 for selection of the item to be presented.

1 8. The method of claim 4, wherein the verification packet further includes
2 a digital signature of contents of the verification packet.

1 9. The method of claim 4, wherein the generating of the key hash result
2 further comprises
3 computing a clock skew by recording a receipt time upon which the verification
4 packet is received and computing a time difference between the receipt time and the
5 local time value;

6 computing the estimated current time at the source corresponding to a current
7 time at a destination based on the clock skew; and

8 performing a cryptographic hash operation on a combination of at least the
9 global identifier and the estimated current time.

1 10. The method of claim 9, wherein the producing of the first time-varying
2 item includes accessing an entry of a lookup table using the key hash result and
3 recovering contents of the entry as the first time-varying item.

1 11. The method of claim 9, wherein the presenting of the first time-varying
2 item further comprises displaying the first time-varying item contemporaneously with a
3 display of the second time-varying item for visual comparison.

1 12. The method of claim 9, wherein the presenting of the first time-varying
2 item further comprises contemporaneous play back of audible sounds associated with
3 both the first and second time-varying items for auditory comparison.

1 13. A software stored in platform readable medium executed by internal
2 circuitry within a computing unit, the software comprising:

3 (a) a first software module to generate a key hash result based on at least a
4 global identifier of a source and an estimated current time at the source;

- (b) a second software module to produce a first time-varying item based on the key hash result; and
- (c) a third software module to present the first time-varying item for comparison with a second time-varying item presented at the source.

14. The software of claim 13, wherein the first, second and third software modules repeatedly generate a new key hash result, produce a new first time-varying item and present the new first time-varying item for each subsequent presentation of a newly produced first time-varying item and compare the newly produced first time-varying item with a newly produced and presented second time-varying item.

15. The software of claim 13 further comprising:

a fourth software module to receive a verification packet from the source, the verification packet including the global identifier of the source and a local time value at which the verification packet was formed at the source.

16. The software of claim 14, wherein the first software module generates the key hash result through computation of a clock skew by recording a receipt time upon which the verification packet is received and computing a time difference between the receipt time and the local time value, computation of the estimated current time at the source corresponding to a current time at a destination using the clock skew, and performance of a cryptographic hash operation on a combination of at least the global identifier and the estimated current time.

1 17. The software of claim 16, wherein the second software module produces
2 the first time-varying item by accessing an entry of a lookup table using the key hash
3 result and recovering contents of the entry as the first time-varying item.

1 18. The method of claim 16, wherein the third software module presents the
2 first time-varying item by displaying the first time-varying item for visual comparison
3 with a display of the second time-varying item intended to be contemporaneous with
4 the display of the first time-varying item.

1 19. A computing unit comprising:

1 a casing;
2 an input/output (I/O) interface;
3 a device that provides sensory data for a user, the device being integrated into
4 the casing; and
5 internal circuitry contained within the casing and controlling information
6 presented by the device, the internal circuitry to generate a key hash result based on a
7 global identifier of a source and an estimated current time at the source.

1 20. The computing unit of claim 19, wherein the internal circuitry is a
2 memory and a processor accessing information from the memory.

1 21. The computing unit of claim 19, wherein the I/O interface is an antenna
2 to receive signals from the source and provide the signals to the internal circuitry for
3 processing.

1 22. The computing unit of claim 19, wherein the I/O interface to receive a
2 verification packet including at least the global identifier and a local time value at
3 which the verification packet was formed prior to transmission to the computing unit.

1 23. The computing unit of claim 22, wherein the internal circuitry generates
2 the key hash result based on the global identifier, the estimated current time at the
3 source and data contained in a data field of the verification packet.

1 24. The computing unit of claim 19, wherein device is a display screen that
2 displays the information being time-varying images.

1 25. The computing unit of claim 23, wherein device is at least one speaker
2 that playback audible sounds which vary in time based on a value of the key hash
3 result.

1 26. The computing unit of claim 23, wherein device is at least a tactile
2 device that produces Braille patterns which vary in time based on a value of the key
3 hash result.

1 27. A network comprising:
2 a first computing unit to (i) transmit successive verification packets each
3 including a static global identifier and a varying local time value realized at the first
4 computing unit during formation of that verification packet, (ii) generate successive
5 first time-varying items based on contents provided within their corresponding
6 verification packet, and (iii) present the first time-varying items in successive fashion;
7 and

8 a second computing unit to (i) receive each verification packet, (ii) compute a
9 clock skew to determine a time difference between the first computing unit and the
10 second computing unit in response to receipt of a first verification packet, (iii) generate
11 successive second time-varying items based on contents provided by their
12 corresponding verification packet, and (iv) present the second time-varying items for
13 comparison with the first time-varying items.

1 28. The network of claim 27, wherein the first computing unit
2 communicates with the second computing unit over a wireless link.

1 29. The network of claim 27, wherein verification that the second
2 computing unit has received the global identifier of the first computing unit when the
3 second time-varying items are presented and changed contemporaneously with the first
4 time-varying items.